

# GENERAL DATA PROTECTION REGULATION (GDPR)

## READINESS WORKSHOP

October 2017

# AGENDA



## **GDPR Overview**

## **Practical Guidance - Building a GDPR Compliance Plan**

## **Q&A**

# GDPR OVERVIEW

# OVERVIEW



## What is GDPR?

- General Data Protection Regulation
- Replaces local EU Data Protection Directive implementations (e.g., in UK the “Data Protection Act”)
- **Starts on May 25, 2018**



## Who is Subject?

- **All organizations that collect and process personal data of EU data subjects** – regardless of size
- No longer applies only to organizations with an office the EU - **is borderless**
- **Applies to data processors** - not just data controllers



## What are the Penalties?

- Up to 20M € or 4% of organization’s annual global turnover, whichever is higher (board attention is now guaranteed)
- Data subjects can claim **compensation for damages** from breaches to their personal data

# PERSONAL DATA



## GDPR Rules

This definition is important because EU data protection law expands the traditional definition of “personal data”. Information that previously did not fall within the traditional definition of "personal data" is now subject to EU data protection law.

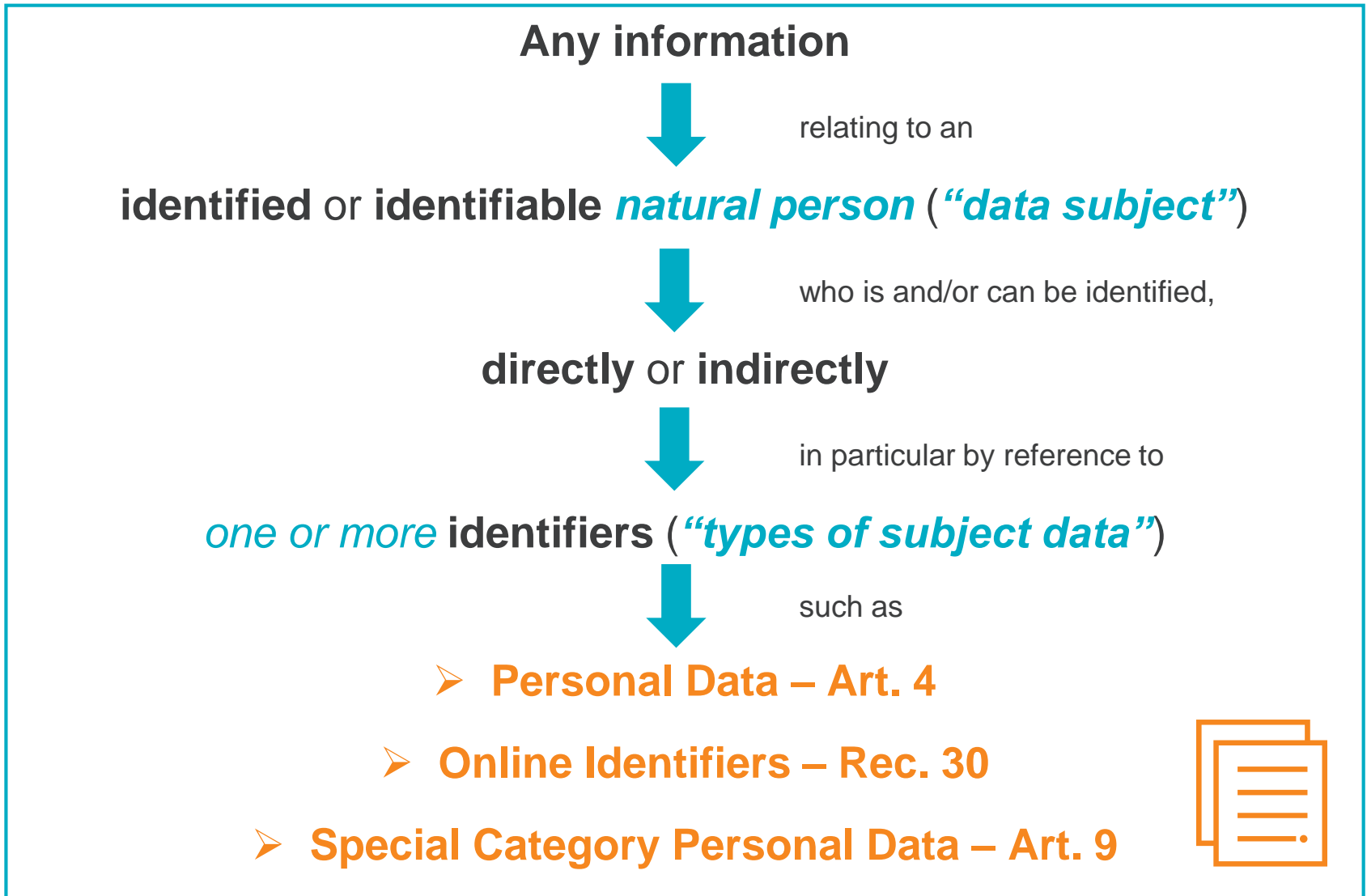


## What is Personal Data?

### Personal Data is defined as:

- Any information relating to an identified or identifiable natural person, “data subject”.
- An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as name, address, online identifiers, location identifiers, financial data, healthcare data, etc.

# PERSONAL DATA DEFINITION



# 3 BUCKETS OF IDENTIFIERS FOR PERSONAL DATA

## IDENTIFIER

### Art. 4

*(Personal Data about the Data Subject)*

Name

Address

Email Address

Passport Number

Financial & Bank Info

Date of Birth

Photographs

Genetic Data

Employee ID

Phone Number

## Online IDENTIFIER

### Rec. 30

*(“...online identifiers [Personal Data] provided by their [Data Subject’s] devices, applications, tools and protocols...”)*

IP addresses, static and dynamic

MAC addresses

Cookies

International Mobile Equipment IDs (IMEI)

International Mobile Subscriber Identity (IMSI)

Advertising IDs

GPS or other location data

Log files

Browser fingerprints

## Special Category IDENTIFIER

### Art. 9

*(Special Categories of Personal Data about the Data Subject)*

Biometric Data  
*(for the purpose of uniquely identifying a natural person)*

Religious or Philosophical Beliefs

Trade Union Memberships

Processing of Genetic Data

Race

Ethnic Origin






Political Opinions

Health

Sex Life

Sexual Orientation

# KEY REQUIREMENTS

	<b>Breach Notification</b>	Requirement to report Privacy breaches to the regulator within <b>72 hours</b> and potentially to the data subject
	<b>Privacy By Design &amp; By Default</b>	Firms must, when introducing new technology, <b>minimize the collection of personal data</b> and ensure that the right security controls are in place throughout all development phases.
	<b>Data Subject's Rights</b>	New rights include the right to erasure (" <b>right to be forgotten</b> ") and the <b>right to data portability</b>
	<b>Consent</b>	Requirement to gain <b>unambiguous consent</b> (i.e. explicit).
	<b>Data Protection Officer (DPO)</b>	<b>DPO required</b> for organizations that conduct regular and systematic monitoring of data subjects on a large scale or process Special Categories of data (e.g., healthcare) on a large scale.



# BUILDING A GDPR COMPLIANCE PLAN

# THE REGULATION



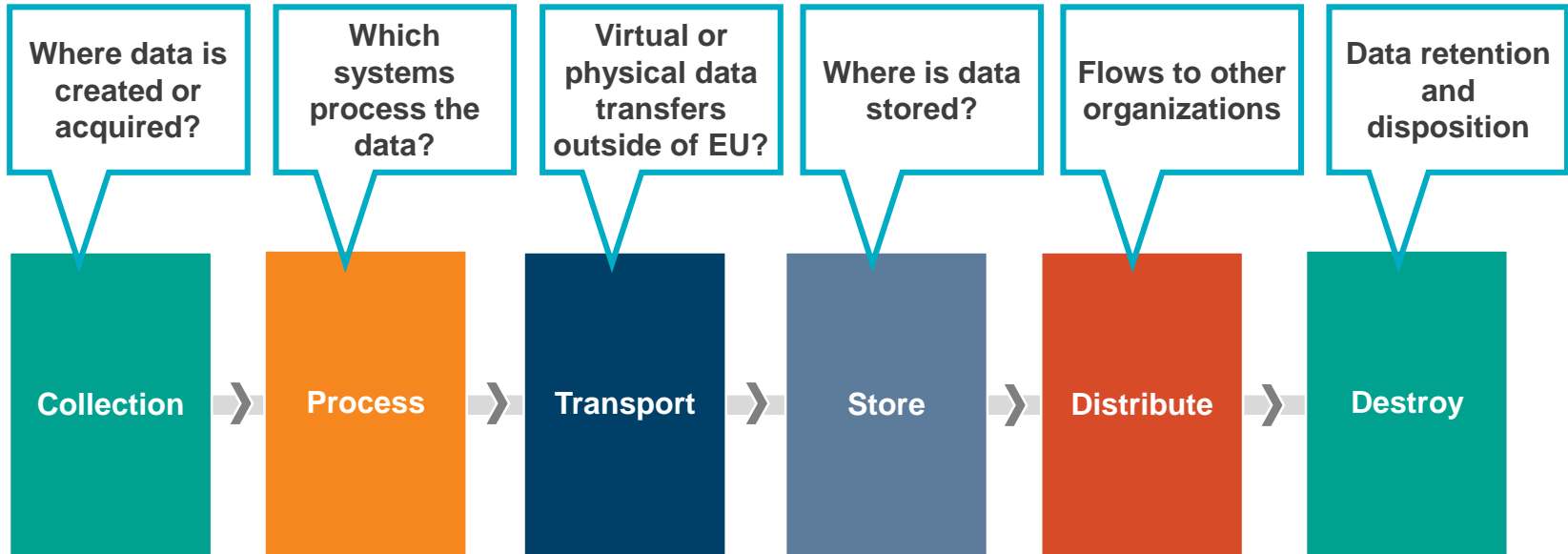
# APPROACH TO GDPR COMPLIANCE



**Phase duration and level of effort** is highly dependent on personal data processed, the size and scope of your environment and process complexity and maturity.



Identify and gather details surrounding processes, systems, and vendors in which personal data is collected, processed, and stored:



In-scope applications and third parties should be prioritized:

- **High Risk** – High probability that a data breach can occur
- **Medium Risk** – Moderate probability that a data breach may occur
- **Low Risk** – Low probability that a data breach may occur



Discovery & Inventory



Readiness Assessment



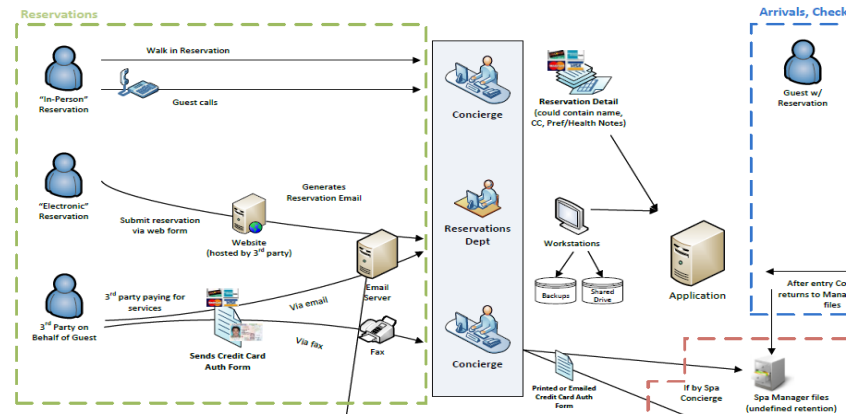
Compliance Remediation



Ongoing Compliance

## Develop a Data Processing Inventory and a Detailed Data Inventory:

- **Data Processing Inventory**, including a record of key processing activities and associated data maps. This high level record of activities includes data subjects, data locations, and the transfer of data to third-parties and across borders. This deliverable will include information required by the supervisory authorities to be available upon request (per Article 30 of the GDPR).
- **Detailed Data Inventory**, including detailed data stores (systems and vendors) information that support key processing activities and how data elements link to each data store. This deliverable will help you achieve the risk assessment requirement of the GDPR to evaluate data processing activities for the rights and freedoms of individuals. Given the risk-based approach advocated by the GDPR, this detailed data inventory will be an important tool when assessing whether, or to what extent, GDPR obligations will apply.

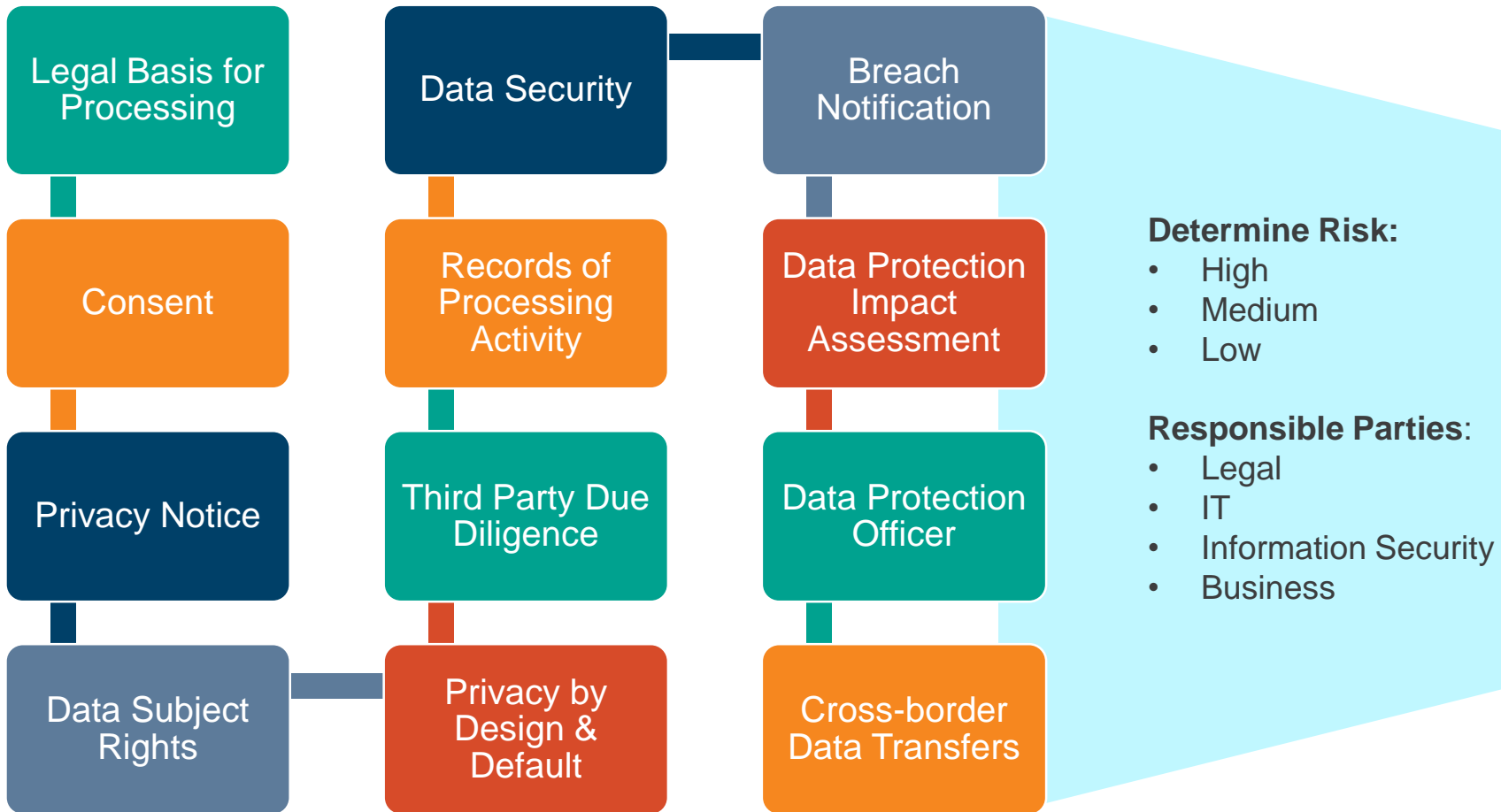


	Name	Address	Date of Birth	Email Address	Phone Number	Home address	Bank Account Details	UK National Insurance Number	Job title	Past Employer References	Internet Usage / Browsing History	Offences / Incidences
Customers	🇺🇸	🇺🇸	🇺🇸	🇺🇸	🇺🇸	🇺🇸			🇬🇧		🇬🇧	🇬🇧
Employees	🇬🇧	🇬🇧	🇬🇧	🇬🇧	🇬🇧		🇬🇧	🇬🇧		🇬🇧	🇬🇧	🇬🇧

🇺🇸 Data originally collected in the US  
 🇬🇧 Data originally collected in the UK



**Evaluate GDPR requirements to identify gaps and develop remediation plans:**





**Data Privacy by Design** – Poor data mapping / lack of priority in design **01**

Accountability (legal, compliance, IT, HR, customer service) **05**

**Rights of Data Subjects** – CRM systems may need major redesign **02**

**Security of Processing** – Formalizing data processing, use of encryption **06**

**Third Party Management** – Data processors, responsibility, contracts **03**

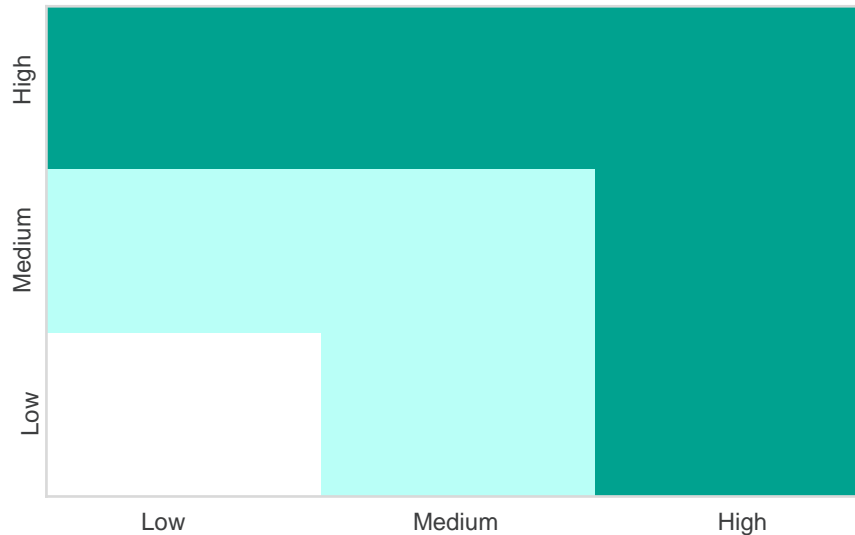
**Data Breach Reporting and Communication** – Process enhancement **07**

**Conditions for Consent** – Using historical data may be a challenge **04**

# COMMON GDPR GAPS



## Heat map Example



### Requirements

1. Legal Basis for Processing
2. Consent
3. Privacy Notice
4. Data Subject Rights
5. Privacy by Design and by Default
6. Third Party Due Diligence
7. Records of Processing Activity
8. Data Security
9. Breach Notification
10. Data Protection Impact Assessment
11. Data Protection Officer
12. Cross-border Data Transfers

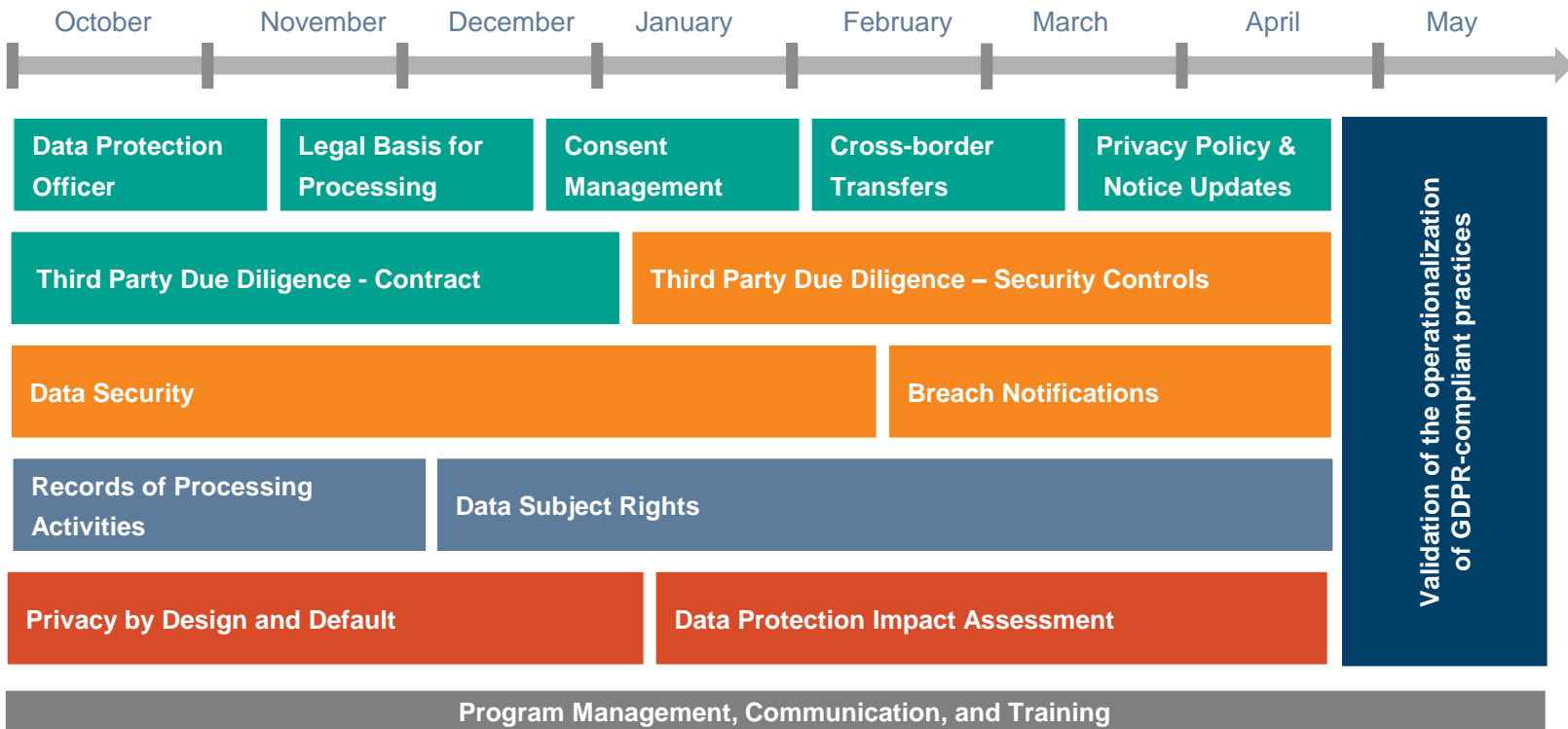
## Determine your Criteria

- **Plot:** Effort, Impact, Duration, Cost, etc.
- **Risk:** High, Medium, Low







# ILLUSTRATIVE COMPLIANCE ROADMAP



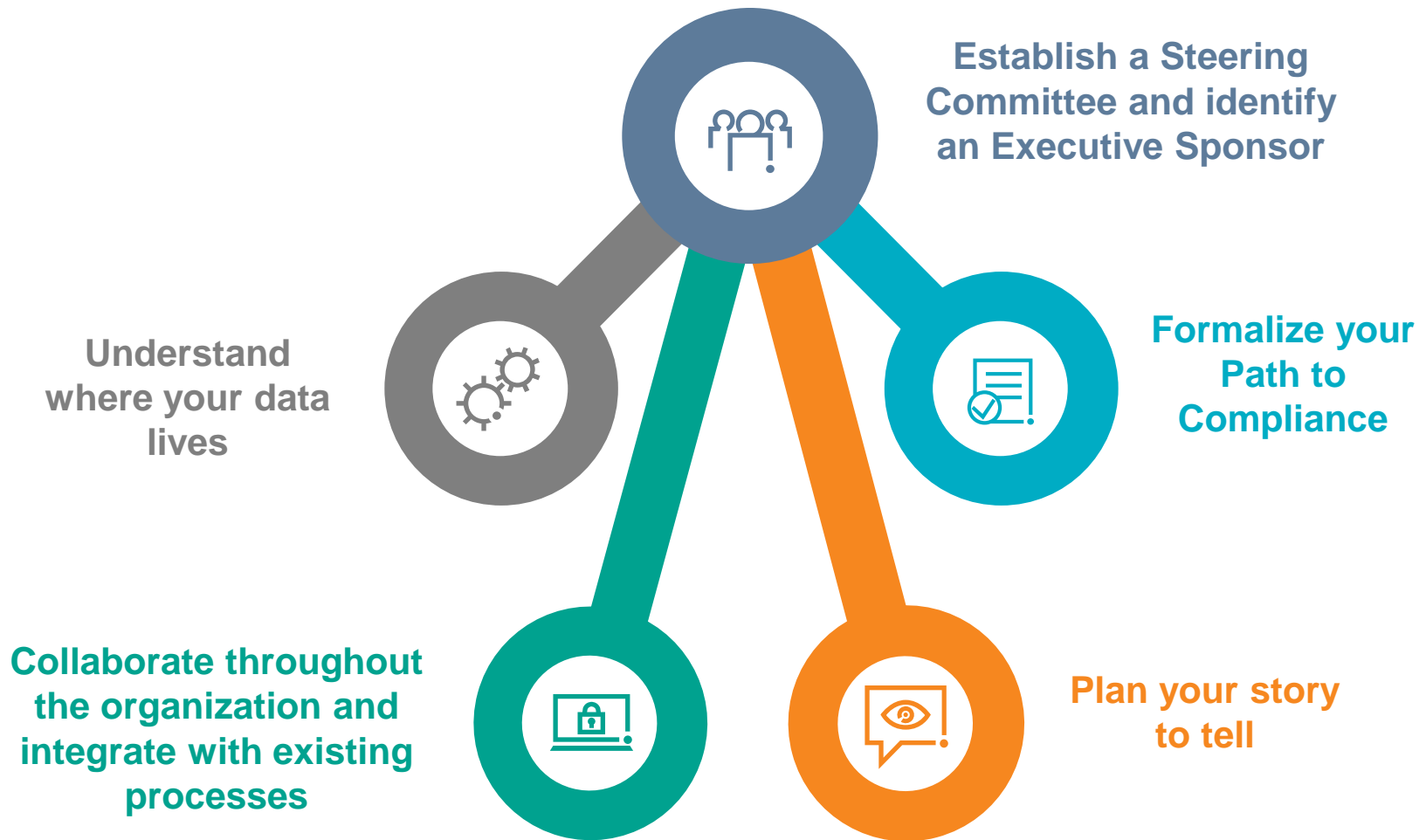
Responsible Party: ■ Legal ■ IT ■ Business ■ Information Security



<b>Data Inventory Maintenance</b> 	<b>Documentation &amp; Monitoring</b> 
<ul style="list-style-type: none"> <li>• Assign roles and responsibilities to keep it accurate</li> <li>• Establish a change management process to keep it accurate</li> <li>• Consider data inventory and data mining tools to keep it accurate</li> </ul>	<ul style="list-style-type: none"> <li>• Assign roles and responsibilities to monitor compliance</li> <li>• Control Documentation / Management</li> <li>• Policy Management</li> <li>• Training</li> </ul>

**! GDPR WILL REQUIRE ONGOING VALIDATION AND COMPLIANCE MANAGEMENT PROCESSES**

# FINAL THOUGHTS



# CONNECT WITH US

**Joel Wuesthoff**

**Robert Half Legal**

**Senior Director**

**Joel.Wuesthoff@roberthalflegal.com**



**Connect with Joel on  
LinkedIn**

# AVAILABLE PROTIVITI RESOURCES

## Resources:

- [GDPR Readiness Webinar](#) held in July 2017 and available for [instant replay](#)
- Thought leadership articles available at [www.protiviti.com/GDPR](http://www.protiviti.com/GDPR)

GDPR Flash Report



GDPR Whitepaper



Protiviti's 2017 Security and Privacy Survey



Board Oversight of Cyber Risk



## Hot Topics Blog Posts:

- [GDPR: Developing Your Compliance Program](#)
- [GDPR: Strict New EU Data Privacy Rules Have Global Reach](#)
- [Internal Audit's Role Will Be Key in the GDPR Journey](#)

*Face the Future with Confidence*

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.

protiviti®